11-CV-00222-EXH

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,

Defendants.

Case No. C11-0222 JLR

**MICROSOFT CORPORATION'S APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

****FILED UNDER SEAL****

## INTRODUCTION

Botnets are computer networks made up of tens of thousands and sometimes millions of end-user computers infected with malicious software that puts them under the control of individuals who use them for illegal activities ranging from disseminating enormous volumes of trademark-infringing spam e-mail, to attacking other computers on the Internet, to stealing financial or other personal information. They are nothing less than a plague on the Internet, afflicting end-users, corporations, and governments alike. This action is about disabling one of the largest, most damaging, and notorious botnets operating today—a botnet known as "Rustock"— which is operated by John Does 1-11 ("Defendants").

Plaintiff Microsoft Corporation ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO"), seizure order, and a preliminary injunction to halt Rustock's



Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

operation and growth. Rustock causes extreme and irreparable injury to Microsoft, its customers, and other members of the public. Rustock illegally infects Internet users' computers with malicious software ("malware") that allows Defendants to illegally control the Rustock-infected end-user computers and use them for a variety of illicit activities, including sending out *billions* of spam e-mail messages that infringe the trademarks of Microsoft and numerous other companies, promoting the sale and distribution of counterfeit pharmaceuticals, advance-fee fraud schemes, and other similar fraudulent scams.

The requested TRO directs the disabling and seizing of Rustock's command and control server software, which operates from and through the Internet Protocol (IP) addresses and Internet domains listed in Appendices A and B to the Complaint. *Ex parte* relief is essential because if Defendants are given prior notice they will be able to destroy, move, conceal or otherwise make inaccessible both the facilities through which they direct Rustock and the primary evidence of their unlawful conduct, rendering further prosecution of this lawsuit entirely fruitless. It is critically important that disabling the IP addresses and domains happens as simultaneously as possible or else the harm will continue.

In a recent analogous case concerning "Waledac", another dangerous botnet, the District Court for the Eastern District of Virginia, Judge Brinkema presiding, addressed exactly this risk by adopting the following approach, which is also appropriate here:

1) the Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure and stop the irreparable harm being inflicted on Microsoft and the public, including Microsoft's customers;

2) immediately after implementing the TRO, Microsoft undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on the defendants, including Court-authorized alternative service by e-mail, mail, facsimile, publication and treaty-based means; and

3) after notice, the Court held a preliminary injunction hearing, and granted

the preliminary injunction while the case proceeded, in order to ensure that harm caused by the botnet could not continue during the action.

*See Microsoft v. John Does 1-27*, Case 1:10-cv-00156 (E.D. Va. 2010, Brinkema, J.) (orders attached to the Declaration of Jeffrey L. Cox ("Cox Decl.") ¶¶ 14, 16, Exs. 12, 14).

If the Court grants the relief Microsoft seeks, Microsoft will immediately make a robust effort in accordance with the requirements of Due Process to provide notice of the preliminary injunction hearing and to effect service of process on the Defendants. Microsoft will immediately serve the complaint and all papers in this action to Defendants, using contact information maintained by the third-party hosting companies and domain registrars that host Defendants' command and control infrastructure.

## STATEMENT OF FACTS

### I. RUSTOCK'S ARCHITECTURE PROVIDES A SOPHISTICATED PLATFORM FOR WORLD-WIDE ILLEGAL ACTIVITY

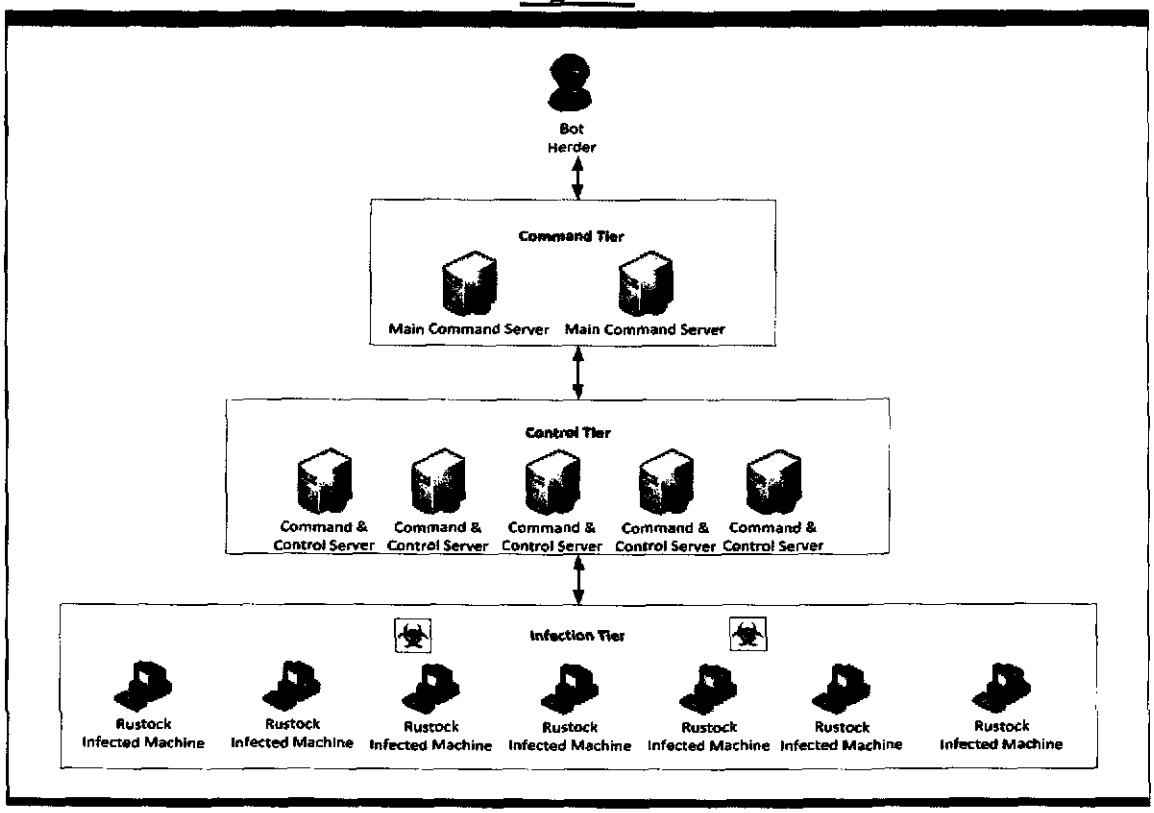
Botnets are networks made up of tens of thousands and sometimes, as is estimated in the case of Rustock, over a million infected end-user computers around the world. Declaration of Thomas J. Campana ("Campana Decl."), ¶¶ 7-8; Declaration of David Dittrich ("Dittrich Decl."); Declaration of Alex Carrol Lanstein ("Lanstein Decl.") ¶ 4. Malicious and criminal actors often use botnets because of their ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them. Dittrich Decl. ¶ 3; Lanstein Decl. ¶ 4. They provide a very efficient general means of controlling huge numbers of computers and targeting any action internally against the contents of those computers or externally against any computer on the Internet. Dittrich Decl. ¶7.

Rustock is a "botnet" and is made up of end-user computers that have been infected, via the Internet, with malicious software ("malware") that places them under the control of Defendants, who use the infected end-user computers for a variety of illegal activities. Campana Decl. ¶ 3; Declaration Of Patrick M. Ford ("Ford Decl.") ¶ 6. Rustock significantly harms Microsoft, its customers, and the public, and if allowed to continue

operating, will only increase the damage it inflicts. Campana Decl. ¶ 2.

In preparation for this action, Microsoft has carefully studied Rustock's architecture, design, and functions. *Id.* ¶ 4. *See* Dittrich Decl. ¶¶ 3-4 (providing background information on typical botnet architectures). The lowest tier of computers in Rustock's architecture, the "Infection Tier," consists of approximately one million Rustock-infected end-user computers. Campana Decl. ¶ 4; Dittrich Decl. ¶ 14. The Infection Tier performs Rustock's daily illegal activities, such as sending out enormous volumes of spam e-mail. Campana Decl. ¶ 4. The middle tier in Rustock's architecture, the "Control Tier," consists of specialized Command and Control Servers that relay commands and information to the Rustock-infected end-user computers in the Infection Tier. *Id.* The top tier in Rustock's architecture, the "Command Tier," though effectively obscured behind the Control Tier, is assumed to be made up of computers that Defendants use to control and direct the Command and Control Servers. *Id.* This hierarchical architecture is depicted in Figure 1. *Id.*

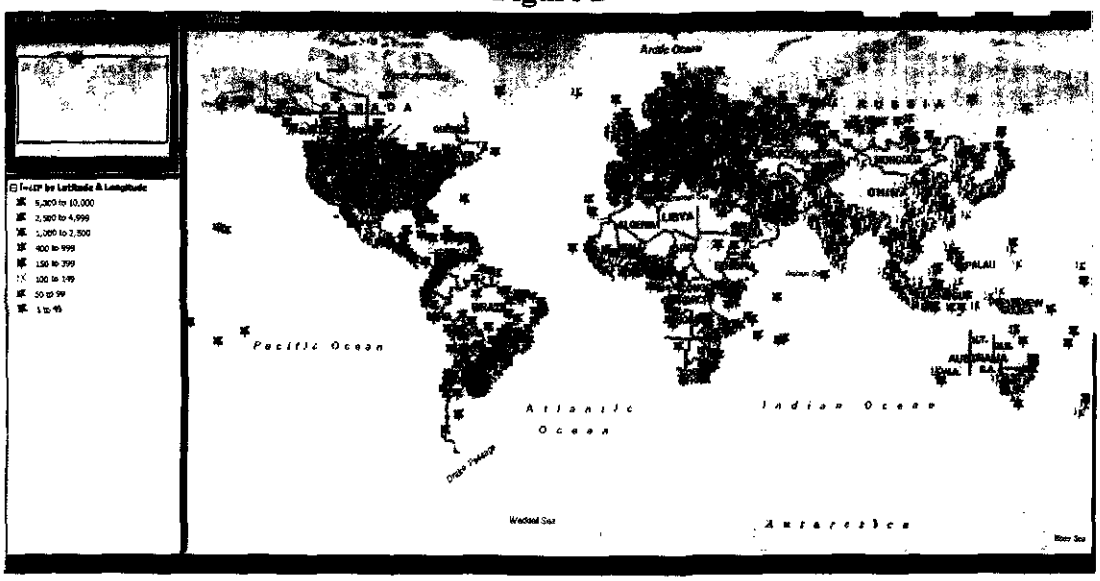
**Figure 1**



1. **The Infection Tier**

The Infection Tier in the Rustock architecture is made up of a large number of Rustock-infected end-user computers of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. Campana Decl. ¶ 6. For example, between January 22, 2011 and February 4, 2011, Microsoft detected Rustock-infected end-user computers connecting to the Internet from over 1,300,000 unique IP addresses. *Id.* ¶ 7. The locations of these addresses world-wide are shown in Figure 2.

**Figure 2**




Analysis by Microsoft and independent researchers indicates that Rustock uses several methods to infect end-user computers. One method involves using malware known as a "Trojan downloader" that infects the end-user computer with Rustock malware, often along with a Devil's brew of other types of malware that Microsoft believes are used to steal the user's confidential information and/or enlist his or her computer in other illegal conduct. *Id.* ¶ 6; Dittrich Decl. ¶¶ 14, 24; Lanstein Decl. ¶¶ 4-5. In general, Defendants are constantly engaged in infecting additional end-user computers with Rustock malware. Campana Decl. ¶ 7. To counter them, numerous software providers and software security firms are constantly engaged in trying to disinfect those computers. *Id.* However, this is a complex task: owners of infected computers would need to undertake a specific investigation to even become



Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

aware of the infection, something many consumers are unable to undertake independently. Campana Decl. ¶ 14.

Reliable analyses estimate that there have been *upwards of one million* Rustock-infected end-user computers in the world. *Id.* ¶¶ 7-8. Defendants direct these Rustock-infected end-user computers to generate and send out a staggering volume of unsolicited bulk e-mail, commonly known as "spam." *Id.* ¶¶ 9-10. *See* Ford Decl. ¶ 5 (defining "spam"). For example, in one 45 minute period on January 25, 2011, Microsoft's investigative team directly observed a single Rustock-infected end-user computer generate approximately 7,500 spam messages. Campana Decl. ¶ 9. Astoundingly, at various times in 2010, Rustock was credited with generating between 20% and 60% of all spam on the Internet. *Id.* ¶ 10. Recent data shows that Rustock's capacity to send out massive volumes of spam remains intact. *Id.*

The vast majority of reviewed samples of Rustock-generated spam promote counterfeit or unapproved generic pharmaceuticals from unlicensed and unregulated on-line drug-sellers. Ford Decl. ¶¶ 7, 26-29, Ex. B; Campana Decl. ¶ 11. A large number of the spam e-mails used the trademarks of a well-known pharmaceutical manufacturer, Pfizer, Inc. Ford Decl. ¶¶ 26-29; Campana Decl. ¶ 11. Still other samples used *both* Pfizer's and Microsoft's trademarks to promote these pharmaceuticals. Campana Decl. ¶ 13, Ex. 12-14. Other Rustock spam samples used Microsoft's "Microsoft," "Hotmail," and "Windows" trademarks to lure recipients into a confidence scam known as "advance fee fraud," in which spammers attempt to convince recipients that they've won a lottery and that they need to send the spammers some amount of money to collect the larger lottery winnings. *Id.* ¶ 12, Exs. 9-10.

Most if not all, owners of Rustock-infected end-user computers are unaware that their computers are infected and operating as part of the Rustock botnet, or that their computers are sending out spam messages. *Id.* ¶ 14.

### 2. The Defendants Command The Rustock-Infected End-User Computers Through The Control Tier

The second level of the botnet, the Control Tier, is comprised of Command and

Control Servers[1] that Defendants have purchased or leased and which they use to relay commands to control the Rustock-infected end-user computers of the Infection Tier. Campana Decl. ¶ 16-17; Dittrich Decl. ¶14-15, 25. There are presently approximately 96 Rustock Command and Control Servers operating on the Internet. Campana Decl. ¶ 16, Appx. A. The number and locations of the Command and Control Servers may change over time, and Microsoft and other security-researchers monitor Rustock to detect these changes. *Id.* ¶ 16; Dittrich Decl. ¶ 15.

The Rustock Command and Control Servers send Rustock-infected end-user computers information and instructions over the Internet that force the Rustock-infected end-user computers to send out spam messages without the knowledge, approval, or involvement of the end-users. Campana Decl. ¶ 18; Dittrich Decl. ¶ 14. The spam sent out by Rustock-infected end-user computers appears to be based on "spam-templates" or resource files that the end-user computers receive from the Rustock Command and Control Servers.[2] Campana Decl. ¶ 19; Dittrich Decl. ¶ 21. Evidence indicates that spam templates or resource files containing Microsoft trademarks are stored on the Rustock Command and Control Servers. Campana Decl. ¶ 19; Dittrich Decl. ¶ 21. The Rustock-infected end-user computers use these templates and resource files to generate the spam that they send out. Dittrich Decl. ¶ 21.

The Rustock Command and Control Servers are located at IP addresses that are associated with computers physically located at 10 data centers or web hosting companies[3] operated by third-parties in the United States. Campana Decl. ¶ 20, Appendix A; Lanstein Decl. ¶ 5-6. Defendants have either purchased or leased these computers, or purchased a

---

[1] The term "Command and Control Servers" refers either to physical server computers in the Command Tier completely dedicated to supporting Rustock, or may be Rustock server software running on computers that might also be running software that is not connected to Rustock.

[2] The term "spam-template" refers to a file that contains what amounts to a pre-written spam message with certain information such as the "To" address and the date represented by variables (essentially, placeholders) that can be replaced with actual information before sending. The term "resource file" refers to a type of file commonly used in software applications that stores strings of text, images, or other information in a way that can be accessed and used by other software programs. Campana Decl. ¶ 19; Dittrich Decl. ¶ 21.

[3] The term "hosting company" refers to a type of company that specializes in offering computer hardware, software, connection to the Internet, technical support, and other services to companies or individuals seeking to have a website or some other presence on the Internet. Campana Decl. ¶ 20.

subscription plan that allows them to run Rustock command and control software on these computers. Campana Decl. ¶ 20.

### 3. The Rustock Control Tier Is Designed To Be Resilient To Attempts To Disable It.

The most vulnerable layer in the Rustock infrastructure is the Control Tier, as the Command and Control Servers can be identified and disconnected from the Internet so that they can no longer communicate with and control Rustock-infected end-user computers. Campana Decl. ¶ 22. *See* Dittrich Decl. ¶ 5 (providing background information on botnet vulnerabilities and defenses). However, Rustock is designed so that it is resilient to attempts to disable the Command and Control Servers. Campana Decl. ¶ 22. For example, over time, the set of IP addresses associated with the Rustock Command and Control Servers changes; some IP addresses fall out of use and new IP addresses are regularly added. *Id.* Because the set of IP addresses used in the Rustock Control Tier is dynamic, it is difficult to disable all Rustock Command and Control Servers operating at any given time. *Id.*

If a Rustock-infected end-user computer is unable to contact any Rustock command and control Server at the IP addresses it is programmed to contact, it will attempt to reestablish its link with the Rustock botnet through two fallback mechanisms. *Id.* ¶ 23. First, each Rustock-infected end-user computer is programmed to attempt to contact a domain[4] called "gbsup.com" if it fails to connect to any of the IP addresses. *Id.* This provides a temporary fallback channel of communication. *Id.*

Next, Rustock-infected end-user computers contain a software routine that enables them to identify new rendezvous addresses on the Internet outside of the current control tier if, in addition to being unable to connect to any of the Command and Control Servers through normal operation, they are also unable to connect with the botnet through the gbsup.com domain. *Id.* ¶ 24. Each Rustock-infected end-user computer will use a customized algorithm to generate 16 random domain names such as "a1msoehl07buqabkp.com" and "gqlpc930epdd2fi.net" per day *Id.* The Rustock-infected

[4] The term "domain" refers to a website with a human-readable name. Each domain is associated with at least one IP address. Campana Decl. ¶ 23.

end-user computers will then begin to attempt to contact these domains for instructions. *Id.* The Defendants, who could generate the same list of domain names by using the same algorithm, would then be able to register these fallback domains and use them to continue to communicate with and control the Rustock-infected end-user computers. Campana Decl. ¶ 24. Additionally, all communications between the Rustock-infected end-user computers and the Command and Control Servers are encrypted, and the malware on the end-user computers is designed to evade tools normally used to investigate and analyze the functioning of the botnet. *Id.* ¶ 25; Dittrich Decl. ¶ 16.

## B. RUSTOCK DIRECTLY INJURES MICROSOFT'S CUSTOMERS

### 1. Overview Of Harm To Microsoft's Customers

Microsoft is a provider of the Windows operating system, Hotmail e-mail services and a variety of other software and services. Campana Decl. ¶ 26. Microsoft has invested substantial resources in developing high-quality products and services. *Id.* Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id.* Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows and Hotmail marks. *Id.*

The activities carried out by the Rustock botnet, described in detail above, and the numerous resulting injuries to the public at large and Microsoft's customers, injure Microsoft and its reputation, brand and goodwill because users subject to the negative effects of the Rustock botnet may incorrectly believe that Microsoft is the source of computer problems caused by the botnet. *Id.*; Dittrich Decl. ¶16-17; Lanstein Decl. ¶ 8. Microsoft is similarly injured because the botnet directs an extraordinary amount of spam e-mail to users of Microsoft's e-mail services. Campana Decl. ¶ 26. *See* Lanstein Decl. ¶ 7. Microsoft and its customers must bear this extraordinary burden and customers may incorrectly believe that

Microsoft is to blame for the spam e-mail. Campana Decl. ¶ 26.

### 2. Rustock's Unauthorized Intrusion Into Microsoft's Customers' Computers

The most direct injury to Microsoft's customers is the installation of the Rustock malware on their computers without their authorization or knowledge. Campana Decl. ¶ 27. Rustock malware is specifically designed to infect and run on computers equipped with the Windows operating system, which is licensed by Microsoft to end-users. *Id.*, Exs. 15-17. End users' computers can become infected with Rustock malware through a variety of mechanisms, some of the most common of which are visiting an infected website where a Trojan downloader designed to download Rustock is staged, or opening an attachment to an e-mail. Campana Decl. ¶ 27.

The installation of Rustock malware in and of itself damages the user's computer and the Windows operating system on the user's computer. *Id.* ¶ 28. During the infection of an end-user's computer, Rustock malware makes changes at the deepest and most sensitive levels of the computer's operating system including the kernel, registry, and systems files. *Id.* It installs its own kernel mode-driver and intercepts and processes various Windows driver-requests. It alters the behavior of various Windows operating system routines by manipulating various registry key settings. *Id.* It replaces Windows files with files of the same name that contain the Rustock malware. *Id.* It installs software that it needs to generate spam and to communicate with the Rustock Command and Control Servers. *Id.* Microsoft's customers whose computers are infected with Rustock malware are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operating system, destabilize it, and which result in the customers' computers being forcibly drafted into the botnet. *Id.*; Dittrich Decl. ¶ 16.

Customers are usually unaware of the fact that their computers are infected and have become part of the Rustock botnet. Campana Decl. ¶ 29. Even if aware of the infection, they lack the technical resources or skills to solve the problem, allowing their computers to be misused indefinitely. *Id.*; Lanstein Decl. ¶ 7. Even with professional assistance, cleaning

a Rustock-infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. Campana Decl. ¶ 29, Exs. 18-24; Lanstein Decl. ¶ 7.

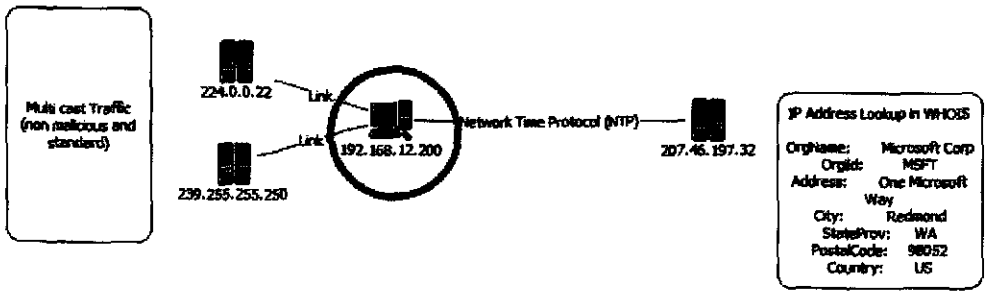
### 3. Microsoft Customers' Computers Are Used in Criminal Activity

Once infected with Rustock malware, the end-user's computer is under the control of the Defendants and used by them for illegal activities. Dittrich Decl. ¶¶ 16, 22. *See also id.* ¶¶ 7-13 (providing background on botnet illegal activities). The primary function of a Rustock-infected end-user computer is to send out a very large quantity of illegal spam e-mail each day of its operation. *See* page 6:4-11, *supra*; Campana Decl. ¶ 31. Furthermore, the spam e-mails sent out by Rustock-infected end-user computers illegally infringe the trademarks of Microsoft and other companies. *See* page 6:14-21, *supra*; Campana Decl. ¶ 31. Rustock spam promotes pharmaceutical products that have been shown to be counterfeit, unlicensed, and potentially dangerous to purchasers. *See* page 6:12-14, *supra*; Campana Decl. ¶ 31; Ford Decl. ¶¶ 26-29. Customers are harmed by having their computers engaged in these illegal, harmful, and potentially criminal activities.

### 4. Microsoft's Customers' Computer-Resources Are Utilized for Illicit Purposes

A Rustock-infected end-user computer's processing power, memory, communications bandwidth, and other resources are used for the high volume of processing, data transfer and connections to the Internet that the Rustock-infected end-user computer engages in. Campana Decl. ¶ 32; Dittrich Decl. ¶ 16. For example, Figure 3 shows the tiny handful of Internet connections made by an uninfected Windows computer (circled) over the course of almost six hours. Campana Decl. ¶ 32.

**Figure 3**

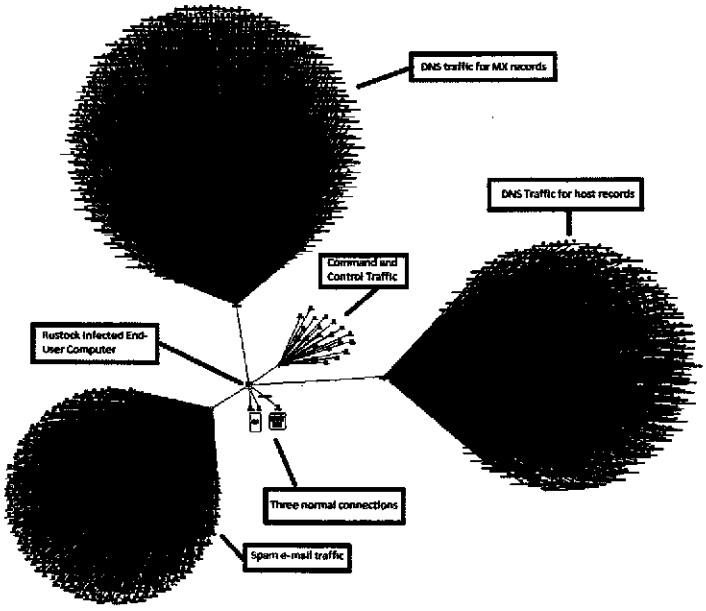





Orrick Herrington & Sutcliffe LLP
*701 5th Avenue, Suite 5600*
Seattle, Washington 98104-7097
tel+1-206-839-4300

In contrast, Figure 4, *infra*, shows the enormous number of Internet connections made in a mere 24 minutes by a Rustock-infected end-user computer. *Id.* ¶ 33. The Rustock-infected end-user computer made the three normal connections of the baseline computer, but in addition, it performed 1406 unique lookups for various DNS "A" hosts on the Internet, 2238 unique lookups for DNS "MX" records for mail servers on the Internet, attempted to send 2310 spam e-mails to 1376 e-mail servers on the Internet, including to a number of Hotmail and MSN e-mail account customers; and in addition made 22 connections to Command and Control Servers on the Internet. Campana Decl. ¶ 33. The computing power and resources devoted to Rustock's nefarious activities are unavailable for the customer's legitimate uses.

**Figure 4**




## 5. Microsoft Customers Are Directly Targeted by Rustock's Spam Campaigns

Microsoft customers are also targeted by Rustock spam campaigns. *Id.* ¶ 34. For example, during the four-day period between October 26, 2010 and October 29, 2010, Rustock-infected end-user computers sent approximately 34 million e-mails to roughly 50 million Hotmail accounts, resulting in an average of approximately eight million spam e-mails per day, providing a good approximation of the total amount of Rustock spam sent to

Hotmail customer accounts on any given day. *Id.* ¶ 34. Approximately 450,000 of these e-mails got through Microsoft's spam filters and reached Microsoft's Hotmail customers. *Id.* ¶34. The very large amount of spam reaching Microsoft's Hotmail customers frustrates them and diminishes their regard for Hotmail and Microsoft. *Id.* ¶ 35, Exs. 25-39. Aside from the harm done to Microsoft Hotmail customers resulting from the sheer volume of Rustock spam bombarding their Hotmail accounts, Rustock's spam attempts to lure them into confidence schemes hatched by the spammers or other activities that will lead to further potential injury, such as purchasing counterfeit or unapproved pharmaceuticals on the Internet. Campana Decl. ¶ 36; Ford Decl. ¶8.

Pharmaceutical counterfeiting, heavily promoted by Rustock, is, in essence, a crime of fraud, trick, and deceit. Ford Decl. ¶ 10. Counterfeiters deceive patients into believing that the products they offer are safe and effective medicines from trusted pharmaceutical companies such as Pfizer, upon whose integrity they have relied to receive medicines that permit them to live happier and healthier lives. *Id.* ¶ 10. In reality, however, counterfeit pharmaceutical products place human lives at grave risk. *Id.* ¶¶ 10-13. And patients who order pharmaceuticals online in response to spam e-mail promotions are particularly likely to place their health at risk. *Id.* ¶¶ 18-22.

## C. RUSTOCK DIRECTLY INJURES MICROSOFT

### 1. Microsoft Pays The High Cost Of Dealing With Rustock Spam

38. Microsoft, as a provider of online e-mail services such as Hotmail, must maintain spam filters to stop Rustock spam from reaching its customers. Campana Decl. ¶ 38. Rustock was acknowledged as the largest known spam botnet in the world at its 2010 peak, with an estimated capacity to send 46 billion spam e-mails per day, including to users of Microsoft's Hotmail e-mail service. *Id.* ¶ 38, Ex. 2, p. 3. Known as the "King of Spam" in the Internet security community at that time, Rustock was estimated to disseminate approximately 40 percent of the world's spam e-mail. *Id.* ¶ 38, Ex. 3, p. 1. While the volume of spam attributed to Rustock fluctuates over time, recent data shows that Rustock is continuing in 2011 as a major contributor of spam on the Internet. Campana Decl. ¶ 38. As

discussed on page 12:23-13:3, *supra*, Microsoft Hotmail systems are the target of a substantial volume of Rustock spam. The sending of vast amounts of spam e-mail to Microsoft's Hotmail e-mail services imposes a burden on Microsoft's Hotmail systems, and requires Microsoft to expend substantial resources in an attempt to defend against and mitigate its effects. *Id.* ¶ 39. *See* Lanstein Decl. ¶ 7 (estimating that, with Rustock generating approximately half the world's spam [as was estimated to be the case for part of 2010], and with 90-95% of enterprise e-mail being spam, "it's not an exaggeration to say that an enterprise would need to deploy about half the mail processing power if Rustock did not exist").

### 2. Microsoft Pays The High Cost Of Assisting Customers Whose Computers Are Infected By Rustock

Additionally, Microsoft devotes significant computing and human resources to combating Rustock infections and helping customers determine whether or not their computers are infected, and if so, cleaning them. Campana Decl. ¶ 40; *See, e.g.*, Lanstein ¶ 7 (estimating, conservatively, two person hours of effort to clean Rustock off of a single computer). Customers' frustration with having to deal with Rustock infections on their computers, discussed on page 10:11-11:2, *supra*, diminishes their regard for Windows and Microsoft, and tarnishes Microsoft's reputation and goodwill. Campana Decl. ¶ 40; Dittrich Decl. ¶16-17; Lanstein ¶ 8.

## D. TURNING OFF THE IP ADDRESSES AND DOMAINS CONTROLLING RUSTOCK WITHOUT FIRST INFORMING THE DEFENDANTS IS THE ONLY WAY TO PREVENT THE INJURY

If given advance notice of any attempt to disable Rustock by disconnecting the IP addresses and domains through which Rustock operates, the Defendants would take measures to keep Rustock alive by migrating the command and control infrastructure to new IP addresses and domains. Campana Decl. ¶ 42. As discussed on pages 8:8-9:8, *supra*, Rustock is designed to withstand technical counter-measures through various means:

a. it has an extensive Control Tier, giving each Rustock-infected end-user computer multiple points of contact with the botnet;

b. it changes the IP addresses of its Command and Control Servers over time;

c. it provides the Rustock-infected end-user computers with a fallback domain, gbsup.com; and

d. both the Rustock-infected end-user computers and Rustock's Defendants are able to generate an alternate list of fallback rendezvous domains should the Rustock-infected end-user computers be unable to communicate with the Command and Control Servers.

Therefore, a piecemeal approach to disconnecting Rustock's Command and Control Servers will fail. Campana Decl. ¶ 42. If less than all of the Command and Control Servers are taken offline simultaneously, and if any of the fallback mechanisms remain viable, the Rustock-infected end-user computers will be able to migrate to the remaining Command and Control Servers or to new command and control servers. Campana Decl. ¶ 42; Lanstein Decl. ¶ 9.

In one previous instance in which an attempt was made to defeat the Rustock botnet by severing communications between the Control Tier and the Rustock-infected end-user computers, the Defendants managed to migrate the botnet's Command and Control Servers to new IP addresses. Campana Decl. ¶ 43. The Rustock-infected end-user computers were then directed to the new IP addresses. *Id.* ¶43. In other prior instances where security experts or the United States government attempted to curb injury caused by botnets, but inadvertently allowed the Defendants to receive notice, the Defendants also immediately moved the botnet command and control infrastructure to entirely new locations, enabling the botnet to continue its operations while also destroying and/or concealing evidence of the botnet's operations. *Id.* ¶ 44; Lanstein Decl. ¶ 9.

The only way to suspend the injury caused by Rustock is to:

a. order upstream network providers to disable the IP addresses;

b. order the relevant hosting companies to disable the IP addresses;

c. order that the content stored on the Command and Control Servers be made inaccessible and to disable any and all "backup" systems, arrangements or

services;

d. order the hosting companies to suspend all services to the bot-herders, to not warn or provide assistance to the bot-herders, and to not enable any circumvention of the order; and

e. order that any effort by the Rustock bot-herders to control or register existing or new backup domains be blocked. Campana Decl. ¶ 45; Dittrich Decl. ¶ 15, 25.

Of particular importance is that the requested actions be closely coordinated, such that the malicious Command and Control IP addresses and domains, in various locations, are turned off simultaneously. Campana Decl. ¶ 46; Dittrich Decl. ¶ 26. If there is delay between disabling Rustock Command and Control servers in the various locations, the Rustock bot-herders may become aware of this action, access the servers in the location that is delayed and move the botnet command and control tier to new, unidentified servers/locations. Campana Decl. ¶ 46; Dittrich Decl. ¶ 27-28.

Some of the IP addresses identified as the addresses of Rustock Command and Control Servers also support domains (i.e., websites) that have not been linked to the Rustock botnet. Campana Decl. ¶ 47. Disconnecting the IP address from the Internet will disconnect these domains. *Id.* However, if appropriate steps are taken to promptly move these domains to new IP addresses, this will have only a negligible impact on these domains. *Id.*

## II. LEGAL ARGUMENT

Microsoft seeks an *ex parte* TRO, seizure order and a preliminary injunction pursuant to Federal Rule of Civil Procedure 65, Section 1116 of the Lanham Act and the court's inherent equitable authority to prevent compounding the harm caused by the Rustock botnet and to maintain the *status quo* by ensuring that evidence of Defendants' misconduct is preserved during the pendency of this case. As discussed below, Microsoft's requested relief is warranted here.

### A. An *Ex Parte* TRO And Preliminary Injunction Disabling The Command And Control Servers Operating The Rustock Botnet Is Warranted

Microsoft seeks a TRO and preliminary injunction pursuant to Rule 65(b) to disable the Command and Control Servers operating the Rustock Botnet. To be eligible for preliminary equitable relief, the movant must establish (1) a likelihood of success on the merits; (2) that it is likely to suffer irreparable harm in the absence of preliminary relief; (3) that the balance of hardships tip in favor of granting the requested relief; and (4) that injunctive relief is in the public interest. *See Winter v. NRDC, Inc.*, 129 S. Ct. 365, 374-76 (2008). The standard is a flexible one and, in the Ninth Circuit, preliminary equitable relief is warranted when the movant demonstrates that serious questions going to the merits are raised and the balance of hardships tips sharply in the movant's favor, assuming of course, that the other two *Winter* factors are met. *Alliance for the Wild Rockies v. Cottrell*, 613 F.3d 960, 964-68 (9th Cir. 2010).

The relief requested by Microsoft is warranted. There is a very high likelihood that Microsoft will succeed on the merits. The Rustock botnet's sending of millions of spam e-mails *each day* through Microsoft's services and to its customers, the unlawful intrusion, and the deceptive use of Microsoft's brands violates the Computer Fraud & Abuse Act, the CAN-SPAM Act, and the Lanham Act. In addition, it is deceptive, misleading and tortious conduct in violation of Washington State law. Microsoft and the public, including Microsoft's customers, will be irreparably harmed if the botnet continues to operate through the 96 Command and Control Servers at issue in this motion.

At the same time, if the TRO, seizure order and preliminary injunction is issued, no legitimate interests of the Defendants will be harmed, and the effect on third-parties (hosting companies and the owners/operators of non-Rustock domains sharing the same IP addresses) will be negligible and short-lived. The public interest also weighs heavily in favor of relief because the same injury inflicted on Microsoft and its customers by the Rustock botnet is also visited on many other U.S. computer users and companies. Accordingly, the relief Microsoft requests is warranted.



Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

### 1. Microsoft Is Likely To Succeed On The Merits On Each Of Its Claims

Microsoft is likely to succeed on the merits of its claims and as such, its request for a TRO and a preliminary injunction should be granted. The Complaint sets forth the following statutory and common law claims: (1) violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) violations of the CAN-SPAM Act (15 U.S.C. § 7704), (3) trademark infringement under the Lanham Act (15 U.S.C. § 1114), (4) false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)), (5) trademark dilution under the Lanham Act (15 U.S.C. 1125(c)), (6) trespass to chattels / computer trespass, (7) conversion, and (8) unjust enrichment.

#### a. Defendants' Violations Of The Computer Fraud And Abuse Act

The Computer Fraud and Abuse Act ("CFAA") penalizes, *inter alia*, a party that:

- intentionally accesses a protected computer[5] without authorization, and as a result of such conduct, causes damage. 18 U.S.C. § 1030(a)(5)(C); or
- intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer. (18 U.S.C. § 1030(a)(2)(C)); or
- knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer. (18 U.S.C. § 1030(a)(5)(A)).

Microsoft's Hotmail servers – "protected computers" under the CFAA – are accessed without authorization and burdened by the sending of an enormous amount of spam e-mail to Hotmail user accounts. This is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See e.g. Hotmail Corp. v. Van$ Money Pie Inc.*, 47 U.S.P.Q.2d 1020, 1025-26 (N.D. Cal. 1998) (granting preliminary injunction under CFAA where defendant sent spam e-mail to Hotmail subscribers without their authorization);

[5] A "protected computer" is a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States." 18 U.S.C. § 1030(e)(2)(B).

*Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (granting a TRO under CFAA where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users).[6]

Microsoft is therefore likely to succeed on the merits of its Computer Fraud & Abuse Act claims against the unlawful intrusion, dissemination of spam e-mail and associated misconduct carried out by the Rustock botnet.

**b. Defendants' CAN-SPAM Act Violations**

The CAN-SPAM Act prohibits, among other acts, initiation of a transmission of a commercial electronic mail message "that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). Here, the Rustock botnet automatically sends e-mails containing false "header" information (*i.e.* originating sender, IP address, etc.) making the e-mails appear to originate from addresses purporting to be associated with Microsoft, or other false addresses, thereby disguising their origin with the purpose of misleading recipients and evading detection. *See* page 6:12-22, *supra*. This is precisely what CAN-SPAM prohibits. *See Gordon v. Virtumundo, Inc.*, 575 F.3d 1040 (9th Cir. 2009) ("[T]he CAN-SPAM Act prohibits such practices as transmitting messages with 'deceptive subjective headings' or 'header information that is materially false or materially misleading.'"). Microsoft is therefore likely to succeed on the merits of its CAN-SPAM Act claim.

**c. Defendants' Lanham Act Violations**

Section 1114(1) of the Lanham Act prohibits the use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services, where such use is likely to cause confusion or mistake, or to deceive. The Rustock botnet distributes copies of Microsoft's registered, famous and distinctive

---

[6] Indeed, in recent years botnet operators who disseminate code that intrudes upon user computers, collects personal information and causes injury have been indicted and convicted criminally under the Computer Fraud & Abuse Act. *See* Cox Decl. ¶ ¶ 18-19, Exs. 16-17 (Indictment of Jeanson James Ancheta), 11 (Sentencing of Jeanson James Ancheta).

"Microsoft" trademark in the headers of unsolicited, spam e-mails, which deceive the recipients, causing them to mistakenly associate Microsoft with this activity. *See* page 6:12-22, *supra*. Defendants' creation and use of counterfeit trademarks is likely to cause confusion or mistake and to deceive consumers. *See* page 6:12-22, *supra*. This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits. *Brookfield Communs. v. W. Coasts Entm't Corp.*, 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (entering preliminary injunction under Lanham Act §1114 for infringement of trademark in software and website code).

The Lanham Act also prohibits use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a). Again, the Rustock botnet's misleading and false uses of the "Microsoft," "Windows," and "Hotmail" trademarks causes confusion and mistake as to Microsoft's affiliation with the malicious conduct carried out by the botnet. This activity is a clear violation of Lanham Act § 1125(a) and Microsoft is likely to succeed on the merits. *See Brookfield Communs. v. W. Coasts Entm't Corp.*, 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp.*, 47 U.S.P.Q.2d at 1024, 1025-26 (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin); *America Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a)).

The Lanham Act further provides that the owner of a famous, distinctive mark "shall be entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark..." 15 U.S.C. § 1125(c). Here, the Rustock botnet's misuse of Microsoft's famous marks in connection with malicious conduct aimed at Microsoft's customers and the public dilutes the famous marks

by tarnishment and by blurring consumers' associations with the marks. Again, this is a clear violation of Lanham Act § 1125(c), and Microsoft is likely to succeed on the merits. *See e.g. Hotmail Corp.*, 47 U.S.P.Q.2d at 1024, 1025-26; (spam e-mail with purported "from" addresses including plaintiff's trademarks constituted dilution); *America Online*, 24 F. Supp. 2d at 552 (same).

**d. Trespass to Chattels/Conversion**

A trespass to chattels occurs where there is: "(1) an act that interferes with a person's right of possession in the property; (2) intent to perform the act bringing about the interference; (3) causation; and (4) damages." *Barr v. City of Roslyn*, 2010 U.S. Dist. LEXIS 5541 at *6-7 (E.D. Wash. 2010). Similarly, "conversion is the act of willfully interfering with any personal property without lawful justification, which causes the person entitled to possession to be deprived of that possession." *Id.*

The unauthorized installation of software onto and subsequent control over Microsoft's licensed Windows operating system software and computers of customers interferes with and causes injury to the value of those properties. Thus, this conduct is an illegal trespass and also constitutes conversion. *See In re Marriage of Langham*, 153 Wn.2d 553, 566 (Wash. 2005) (conversion of intangible property); *Kremen v. Cohen*, 337 F.3d 1024, 1034 (9th Cir. Cal. 2003) (recognizing that hacking into a computer system and injuring data supports a conversion claim); *Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868 (E.D. Va. 2003) (granting TRO and preliminary injunction where defendant hacked computers and obtained proprietary information holding "there is a likelihood that the two alleged attacks that [Plaintiff] traced to Defendants were designed to intermeddle with personal property in the rightful possession of Plaintiff."); *see also State v. Riley*, 121 Wn. 2d 22, 32 (Wash. 1993) (affirming conviction for "computer trespass" under Washington law for defendant's "hacking activity").

Likewise, unauthorized intrusion into Microsoft's servers providing the Hotmail service, by sending Hotmail users vast quantities of spam e-mail, injures Microsoft's property and constitutes a trespass. *See e.g. State v. Heckel*, 143 Wn. 2d 824, 834 (Wash.

2001) (spam e-mail burdens possessory interest in computers; recognizing trespass to chattels, citing *AOL v. IMS*); *America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (senders of spam e-mail committed trespass when they "caused contact with [plaintiff's] computer network ... and ... injured [plaintiff's] business goodwill and diminished the value of its possessory interest in its computer network.")

**e. Unjust Enrichment**

The elements of a claim of unjust enrichment are (1) the plaintiff's conferring of a benefit on the defendant, (2) the defendant's knowledge of the conferring of the benefit, and (3) the defendant's acceptance or retention of the benefit under circumstances that "make it inequitable for the defendant to retain the benefit without paying for its value." *Ballie Commc'ns Ltd. v. Trend Bus. Sys. Inc.*, 61 Wn.App. 151, 160, 810 P.2d 12 (1991). Here, without authorization, the parties controlling the botnet have taken the benefit of Microsoft's servers, networks and e-mail services, its licensed Windows operating system software and the computers of Microsoft's customers. Defendants have done so by improperly infecting these computers, and causing them to send and receive, collectively billions of spam e-mails, including e-mail that infringes famous Microsoft trademarks. Defendants have profited from this activity. Thus, it is certainly inequitable for the parties controlling the botnet to retain this benefit. Microsoft is likely to succeed on the merits.

**2. Irreparable Harm Will Result Unless a TRO and Preliminary Injunction Are Granted**

Continued operation of the Rustock botnet irreparably harms Microsoft, its customers and the public. No monetary remedy could repair the harm to Microsoft or its customers if the botnet were permitted to continue operating and expanding. Federal courts in the two civil cases to date addressing botnets concluded that the "immediate and irreparable harm" to consumers from "botnet command and control servers, spyware, viruses, Trojans, and phishing-related sites; and configuring, deploying and operating botnets," warranted an *ex parte* TRO and preliminary injunction. *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) at Dkt. 13, pgs. 2-4; *FTC v. Pricewert LLC et al.*, Case



Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

No. 09-2407 (N.D. Cal., Whyte J.) at Dkt. 12, pg. 2 (June 2, 2009 *Ex Parte* Temporary Restraining Order and Order to Show Cause) and Dkt. 37, pgs. 2-3 (June 15, 2009 Preliminary Injunction), submitted herewith at Cox Decl. ¶¶ 14, 16, 17, Exs. 12, 14, 15. Specifically, the district court in *Microsoft Corporation v. John Does 1-27,* acknowledged the substantial irreparable harm botnets cause Microsoft, its customers and Internet users generally. Cox Decl. at ¶ 14, Ex. 12.

Microsoft and the public face the same irreparable harm caused by the Rustock botnet. Thus, entry of an *ex parte* TRO disabling the IP addresses from and through which the Rustock Command and Control Servers operate and an Order to Show Cause why a preliminary injunction should not issue is warranted. Microsoft is irreparably injured because the problems of spam e-mail and system performance degradation caused by the botnet are improperly attributed to Microsoft. *See* page 9: 21--25. Microsoft's customers may migrate to other platforms, products or services in the belief that Microsoft is the cause of the problems. Once such a switch occurs, given the costs of switching platforms and the uncertainty caused by the botnet in the first place, there is a very high risk that those customers will not return to Microsoft. As the botnet continues to grow, this harm is compounded. This type of brand related injury and customer harm is most certainly irreparable and is precisely why the relief requested in this motion should be granted. *See Rent-A-Center, Inc. v. Canyon Television and Appliance Rental, Inc.*, 944 F.2d 511, 519-20 (9th Cir. 1984) ("intangible injuries, such as damage to ongoing recruitment efforts and goodwill, qualify as irreparable harm"); *Stuhlbarg Int'l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001) ("threatened loss of prospective customers or goodwill certainly supports a finding of the possibility of irreparable harm").

Further, if the requested relief were not granted, the computers of Microsoft's customers would continue to be infected and the botnet would grow. This injury is irreparable because customers, for the most part, lack the technical knowledge, skills, and ability to remedy the infection or curtail the growth of the botnet. In the absence of the requested relief, Microsoft's customers would remain under constant threat of their



Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

computers being made part of the botnet with the accompanying harmful effects of unauthorized intrusion into and abuse of their computers.

### 3. The Balance Of Hardships Tips Sharply In Microsoft's Favor

Defendants will suffer *no harm* to any legitimate interest if an *ex parte* TRO and preliminary injunction are issued, because it will do no more than preserve the status quo. Disabling the command and control server software, IP addresses, and domains through which the Rustock botnet operates will prevent it from spreading to any additional computers during that time and will preserve the evidence of the botnet's structure and illegal activities. *See* pages 15:23 -16:13, *supra*. Legitimate activity carried on from and through these IP addresses, if any, can be easily and swiftly migrated by the hosting companies to other IP addresses. *See* page 16: 14-18, *supra*. Similarly, there will be only negligible impact on the third-party hosting companies, as the requested relief is carefully tailored to only disable access to a small number of their IP addresses and directs these third parties to take simple steps to assist in preserving evidence. Likewise, the domains at issue have no purpose but to support the botnet.

Conversely, if a TRO and preliminary injunction do not issue, the Rustock botnet will continue to inflict irreparable injury on Microsoft, its customers, and the public. The botnet already includes approximately a million compromised user computers, sending millions of spam e-mails to Hotmail users each day. New users are infected each day, dramatically increasing the botnet's capacity to carry out illegal conduct, compounding the injury to Microsoft and the public.

Simply put, maintaining the status quo by disabling the IP addresses and domains through which the botnet is controlled will not affect any legitimate rights of the Defendants, seeks only narrowly tailored assistance from the third-party hosting companies and domain registrars and registries, and will have a negligible effect on any potential legitimate interests of other third-parties. However, allowing the botnet to grow and continue to harm Microsoft and the public while this action is adjudicated poses grave danger to many legitimate interests.

### 4. The Public Interest Will Be Served By The Issuance Of A TRO And Preliminary Injunction

A TRO and preliminary injunction protects the public interest and not just Microsoft and its own customers because the Rustock botnet poses serious health and safety threats. A large percentage of Rustock spam promotes counterfeit and potentially dangerous and unregulated pharmaceuticals that may cause their recipients serious injuries. *See* pages 6:12-14; 13:9-16, *supra*. Every consumer with access to an e-mail platform and the Internet is at risk of being irreparably injured by the Rustock botnet. Similarly, every company providing e-mail services and websites is at risk of having its systems misused to propagate the botnet.

There is an overwhelming public interest in preserving the status quo and halting the growth of the Rustock botnet while Microsoft proceeds with its claims. Two district courts in the last two years have concluded that "immediate and irreparable harm" will result to the welfare of consumers from "botnet command and control servers" and the malicious conduct carried out through botnets. *See Microsoft v. John Does 1-27,* Dkt. 13 at pg. 2 (Cox Decl. ¶ 14, Ex. 12 (granting *ex parte* TRO); *Federal Trade Commission v. Pricewert LLC et al.*, Dkt. 12 at pg. 2 (Cox Decl. ¶16, Ex. 14 (granting *ex parte* TRO)). Likewise, a TRO and preliminary injunction here will preserve and protect this important public interest. No such protection will be afforded if preliminary relief is denied and, in that event, the malicious actors controlling the Rustock botnet will be able to continue their activities with impunity.

### 5. Only The Requested *Ex Parte* Relief Can Halt The Irreparable Harm To Microsoft And The Public

Absent a TRO granting the relief requested herein, the injury to Microsoft and the public, including Microsoft's customers, will continue unabated, irreparably harming Microsoft's reputation, brand and goodwill. The TRO, moreover, must issue *ex parte* for the relief to be effective at all, and the extraordinary factual circumstances here warrant such relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Teamsters,* 415 U.S. 423, 438-39, 94 S.Ct. 1113 (1974) ("Ex parte temporary restraining

orders are no doubt necessary in certain circumstances....").

**a. If Notice Is Given, The Botnet Will Be Moved And Concealed, Allowing The Harm To Grow And Render Microsoft's Request For Relief Fruitless**

If notice is given prior to issuance of a TRO, the Rustock botnet Command and Control Servers will be moved to different servers, at different IP addresses, in different areas, enabling Defendants controlling the botnet to continue infecting users' computers with malicious software, sending billions of spam e-mails and carrying out other conduct inflicting irreparable injury on Microsoft and the public. Indeed, there is specific evidence that the operators of the Rustock botnet evaded prior enforcement attempts, where they had notice, by moving the Command and Control Servers. *See* page 15:13-17, *supra.* If the botnet's Command and Control Servers are allowed to move, the investigation of the botnet and the illicit activities carried out through it would have to be started anew. Providing notice of the requested TRO will undoubtedly facilitate efforts of the parties controlling the botnet to avoid prosecution.

It is well-established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief "fruitless." *See e.g. Crosby v. Petromed, Inc.,* 2009 U.S. Dist. LEXIS 73419, *5 (E.D. Wash. 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs..."); *In the Matter of Vuitton Et Fils S.A.,* 606 F.2d 1, 4 (2d Cir. 1979) (*per curiam*) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless).

Particularly instructive here is *Microsoft Corporation v. John Does 1-27,* where, in February 2010, a district court issued an *ex parte* TRO and supplemental *ex parte* TRO suspending 276 Internet domains used to control a malicious botnet. *See Microsoft Corporation,* Case No. 1:10-cv-156 (LMB/JFA) (E.D. Va., Brinkema J.) at Dkt. 13, pp. 3-5.

In issuing the *ex parte* TRO, the court acknowledged that:

> There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the domains at issue in Microsoft's TRO Motion and other discovery evidence of Defendants' misconduct available through such domains if the Defendants received advance notice of this action...

*Id.* at ¶ 3.

Also instructive is *FTC v. Pricewert LLC et al.*, where the court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that "Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff's] action." *See FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.) at Dkt. 12, pg. 3 (June 2, 2009 *Ex Parte* Temporary Restraining Order and Order to Show Cause), at Cox Decl., ¶ 16, Ex. 14. Moreover, the court in *Dell, Inc. v. Belgiumdomains, LLC,* 2007 U.S. Dist. Lexis 98676, *4-5 (S.D. Fla. Nov. 21, 2007) issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. *Id.* at *4. In *Dell* the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *5-6.

**b. <u>If Notice Is Given, Evidence Regarding The Botnet Will Be Destroyed, Disturbing The Status Quo</u>**

If notice is given in advance of a TRO, evidence of the botnet will be destroyed. In particular, upon notice, the movement of the botnet command and control software will not only destroy evidence of the botnet's operation, but is also likely to lead to destruction of additional evidence available through that software, such as the identity of infected user computers and other aspects of the system necessary to this litigation. Under such



Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

circumstances, courts have issued *ex parte* TROs. *See AT&T Broadband v. Tech Commc'ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Dell, Inc,* 2007 U.S. Dist. LEXIS 98676 at *4-5; *Little Tor Auto Center v. Exxon Co., U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"). For this reason, the requested *ex parte* TRO is warranted.

**B. Only An *Ex Parte* Seizure Order Can Halt The Irreparable Harm To Microsoft And The Public**

Given Defendants' technological sophistication and expertise in evading enforcement, there is an overwhelming risk that if the most active, current command and control software is not physically isolated on secure media, seized and impounded with the assistance of the United States Marshals Service, Defendants will be able to move the botnet, continue their infringement and continue their related activities causing irreparable harm. Thus, seizure and impoundment of the most active, current command and control software is warranted.

Section 1116(d) of the Lanham Act provides for *ex parte* seizure and impoundment of infringing and counterfeit items, the instrumentalities used to reproduce the infringing and counterfeit articles, and the records documenting the manufacture, sale and receipt of such materials. *See* 15 U.S.C. § 1116(d); *Microsoft v. Jun Yan*, 2010 U.S. Dist. LEXIS 14933, 6-7 (D. Conn. 2010).[7] It is well-established that an *ex parte* seizure order is appropriate where notice would allow defendants to continue their infringement or to destroy, move, hide or otherwise make inaccessible evidence of infringement. *See id.* at *1; *AT&T Broadband v.*

[7] *See also Lorillard Tobacco Co. v. Can-Star (U.S.A.) Inc.*, 2005 U.S. Dist. Lexis 38414, *3-4 (N.D. Ill. 2005) ("an *ex parte* motion to search defendants' residences and seize information concerning their finances is the only manner in which to preserve evidence of the location and extent of their assets..."); *Polo Fashions, Inc. v. Clothes Encounters,* 1984 U.S. Dist. Lexis 18196, *8-9 (N.D. Ill. 1984) (*ex parte* TRO appropriate where evidence "relating to the source and the amounts of such merchandise might disappear and the distributor or source of supply thereof remain undetected ...").

*Tech. Commc'ns., Inc.*, 381 F.3d 1309, 1319 (11th Cir. 2004); *In the Matter of Vuitton Et Fils S.A.*, 606 F.2d at 4. It is also well-settled that courts can impound computers, servers and other electronic data that constitute infringing items, instrumentalities used to carry out infringement or records of infringement. *See e.g., Dell,* 2007 WL 6862341 at *4-5 (issuing an *ex parte* TRO and seizure order under Section 1116(d) that allowed for a forensic analysis of the defendants' computer data for records).

The Lanham Act authorizes an *ex parte* seizure and impoundment order where the court (1) finds no order other than an *ex parte* seizure is adequate to achieve the purpose of Section 1114; (2) the applicant has not publicized the requested seizure; (3) the applicant is likely to succeed in showing the person against whom seizure would be ordered used the counterfeit mark in connection with the sale, offering for sale, or distribution of goods or services; (4) the applicant will suffer irreparable harm; (5) the matter to be seized will be located at the place identified in the application; (6) the balance of hardships tip in favor of seizure; and (7) the persons against whom the seizure would be order or those working in concert with them would destroy, move, hide or otherwise make such matter inaccessible to the court if the applicant provided notice. *See* 15 U.S.C. § 1116(d)(i)-(vii). Each of these criteria is met in this case.

### 1. Only Seizure Of The Botnet Software Can Ensure That The Defendants Will Not Continue Their Activities Or Destroy Or Conceal Evidence

An *ex parte* seizure order of the most active command and control servers is critical to ensure that Defendants cannot continue their deceptive use of Microsoft's trademarks and to ensure that Defendants will not destroy or conceal evidence, all of which would render the further prosecution of this action fruitless. Here, there is substantial evidence that if such command and control software is not physically seized in a highly coordinated manner, Defendants will be able to continue their misleading and illegal use of Microsoft's trademarks in spam e-mails disseminated by Rustock. Indeed, in a prior enforcement attempt, the operators of the Rustock botnet moved the Command and Control Servers during a brief period when connectivity was inadvertently restored, allowing the botnet to

continue harming Microsoft and the public for years. Seizure and impoundment of the command and control software would have avoided this result and is thus warranted in this case, in order to preserve the evidence, thwart Defendants' continued operation of the botnet and protect against inadvertent or intentional acts by any hosting company that would enable Defendants to migrate Rustock's command and control software to new IP addresses and/or destroy evidence of the operation of Rustock.

**2. Microsoft Will Not Publicize The Requested Seizure In Advance**

Other than notifying the United States attorney for the Western District of Washington and the United States Marshals Service in districts where seizure is to be effected, pursuant to Section 1116(d)(2) of the Lanham Act, Microsoft has not and will not publicize the requested seizure until after the requested seizure is carried out. Cox Decl., ¶ 11.

**3. Microsoft Is Likely To Succeed On The Merits Of Its Trademark Infringement Claim**

As discussed, the Command and Control Servers create and send spam e-mail that makes infringing use of counterfeit Microsoft trademarks, in particular the famous and distinctive "Microsoft," "Windows," and "Hotmail" trademarks, in order to deceive users. This constitutes trademark infringement and false designation of origin under Sections 1114 and 1125(a) of the Lanham Act. The Command and Control Servers and software both contain counterfeit trademarks and are instrumentalities used to carry out the infringement. Thus, Microsoft is likely to succeed on the merits and the command and control software is subject to seizure and impoundment under Section 1116(d) of the Lanham Act.

**4. Immediate And Irreparable Injury Will Occur If An *Ex Parte* Seizure Order Does Not Issue**

As discussed above, Microsoft, its customers and the public will continue to suffer irreparable harm if the Rustock botnet is allowed to continue growing through the infringement of Microsoft's trademarks and is allowed to carry out its malicious activities. Each day the Rustock botnet is allowed to operate and grow, it disseminates billions of spam e-mails and infects many end-user computers with its malicious code. As district courts have

recently acknowledged, this unlawful conduct irreparably injures Microsoft, its customers and the public. *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) at Dkt. 13, pgs. 2-5; *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.) at Dkt. 12, pg. 2.

**5. The Material To Be Seized And The Locations To Be Searched Are Identified In The Application**

In its proposed seizure order, Microsoft identifies with specificity the items to be seized and the place where the Command and Control Servers can be found. The proposed order identifies ten data centers and hosting companies, supporting the relevant IP address and domains in up to 19 locations, whose services are being used by Defendants to host the Rustock botnet Command and Control Servers.

As to the materials to be seized, the proposed order directs the U.S. Marshals Service to seize the computers, servers, electronic data storage devices, software, data or media that correspond to the botnet IP addresses assigned to Defendants. This material is readily ascertainable because each IP address corresponds to computers in the hosting companies' possession, custody or control. The proposed order directs the hosting companies to isolate and turn over to the U.S. Marshals Service the botnet software and related content on the computers associated with these IP addresses.

The proposed order also identifies categories of records and documents to be seized or provided, including information relating to the identity of the Defendants using these servers and all logs associated with these servers, all of which is readily ascertainable. This information will enable Microsoft to effect notice and service of process on Defendants. These categories are sufficiently specific to allow the U.S. Marshals Service, the hosting company and third-party forensic experts under contract with Microsoft, to locate the material to be seized without undue burden.

As Microsoft anticipates that some of the material to be seized will be electronic data files, it requests the Court to issue a writ of assistance allowing forensic experts to assist with the identification of the electronic data and media that contain the malicious code. A district

court has the power to issue a writ of assistance that compels third parties with technical skills to assist in the technical implementation of a court's order. *See Dell, Inc.*, 2007 WL 6862341 at *4 (citing to *U.S. v. New York Tel. Co.*, 434 U.S. 159, 176 (1977).

### 6. The Harm To Microsoft And The Public Of Denying The Requested Relief Outweighs The Harm To Any Legitimate Interests Of Defendants

As previously established, if the requested relief is denied, serious and irreparable harm to Microsoft and the public will result. By contrast, Defendants will suffer no harm to any legitimate interest if an *ex parte* TRO and seizure Order issues, as the malicious Rustock command and control code operating from the servers at those IP addresses and domains is used solely to propagate and control the Rustock botnet and not for any legitimate or lawful purpose. Further, as discussed, the impact of the requested relief to the third party hosting companies or domain registrars/registries will be negligible, as the order disables access to only a handful of their customers engaged in illegal conduct and seeks the hosting companies' reasonable assistance in the isolation and seizure of the botnet code. Because each unique IP address or domain is associated with a specific command and control server, identifying and isolating the malicious code onto secure computers should result in only minimal burden to the hosting companies and domain registrars/registries. Microsoft, moreover, will utilize forensic experts to expedite the seizure and further minimize any potential burden. Finally, the impact of the requested relief on any other parties who may host legitimate content, if any, on any of the otherwise malicious IP addresses listed, will also be negligible. Such content can be quickly and readily moved by the relevant hosting provider to another IP address and the owners/operators of the content can be promptly notified of the change in IP address.

### 7. Defendants Are Likely To Destroy, Move, Hide Or Conceal Evidence If They Were Provided Notice

As previously discussed in detail, Defendants are likely to remove the malicious code and relocate it to new servers if they are provided notice. *See* page 15:7-12 *supra*. As such, an *ex parte* seizure order is necessary to prevent Defendants from destroying, concealing or

otherwise making inaccessible the evidence of their unlawful conduct.

### C. Microsoft Will Make Extraordinary Efforts To Provide Notice Of The TRO And The Preliminary Injunction Hearing And To Serve The Complaint

To ensure Due Process, immediately upon entry of the requested *ex parte* TRO, Microsoft will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to the Defendants and to serve the complaint. In order to effect service, the proposed TRO also directs the relevant hosting companies and domain registrars/registries to provide all contact information for the Defendants through which notice may be provided.

The Ninth Circuit permits discovery to determine the identity of unknown defendants. *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980). The party seeking discovery must (1) identify the missing party with sufficient specificity so that the Court can determine that the defendant is a real person or entity who could be sued in federal court; (2) identify all previous steps taken to locate the elusive defendant; (3) establish that its action against the Doe Defendants can withstand a motion to dismiss; and (4) support its request for discovery with reasons justifying the specific discovery requested, as well as identification of a limited number of persons or entities on whom discovery process might be served. *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. 573, 578-79 (N.D. Cal. 1999).

Here, Defendants are real people who have created and now direct the daily operation the Rustock botnet. If identified, they will be amenable to suit in federal court. Microsoft has diligently researched the Rustock botnet, and has identified 96 IP addresses that comprise the command and control tier of the botnet set up by the Defendants. Microsoft's investigation into their identity can progress no further until it gains access to more information related to the identity of the individuals who control the command and control services through those 96 IP addresses. As discussed on pages 18:1-22:18, *supra*, Microsoft's action can withstand a motion to dismiss. Finally, Microsoft's request for information allowing it to identify the Defendants is the only way Microsoft will be able to identify the Defendants, serve them with process, and bring them to justice for the harms

they have inflicted on Microsoft, Microsoft's customer's and the public. Microsoft's requests for contact information will be made only to the hosting companies that provide support for the critical infrastructure of the botnet, and Microsoft seeks only sufficient discovery to allow it to identify them. Therefore, good and compelling cause exists to grant Microsoft leave to conduct Doe discovery.

**Microsoft Will Provide Notice To Defendants By Personal Delivery:** Microsoft has identified 96 IP addresses from which the Rustock command and control software operates, and, pursuant to the TRO, will obtain from the hosting companies and domain registrars/registries any and all physical addresses of the Defendants. Pursuant to Rule 4(e)(2)(A), Microsoft plans to effect formal notice of the preliminary injunction hearing and service of the complaint by hand delivery of the summons, Microsoft's Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the U.S.

**Microsoft Will Provide Notice Through The Hague Convention On Service Abroad:** If physical addresses provided by the data centers/hosting companies and domain registrars/registries are located in foreign jurisdictions, Microsoft will attempt service under international treaties. Pursuant to Rule 4(f)(1), Microsoft is prepared to effect notice of the preliminary injunction hearing and service of the complaint through the Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents ("the Hague Convention") or other relevant judicial assistance treaties. Microsoft will translate the pleadings into the relevant language and immediately request that the respective central authority deliver the summons, Microsoft's Complaint, the instant motion and supporting documents, and any Order issued by this Court to Defendants.

Microsoft anticipates that this means of notice of the preliminary injunction hearing and service of the Complaint could take approximately three to six months to effect service through the respective central authorities. Accordingly, in addition to making every effort to expedite this process, given the irreparable harm and the need for prompt relief, Microsoft and its counsel will also provide notice of the TRO and the preliminary injunction hearing

and will effect service of the Complaint through other means described below.

**Microsoft Will Provide Notice By E-mail, Facsimile And Mail:** Microsoft will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses that Defendants provided to the hosting companies in relation to hosting the command and control software at the Rustock IP addresses, and to the domain registrars/registries. When Defendants registered for hosting services or for domain names, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. *See* Cox Decl., ¶¶ 12-13.

**Microsoft Will Provide Notice To Defendants By Publication:** Microsoft will notify the Defendants of the preliminary injunction hearing and the complaint against their misconduct by publishing the materials on a centrally located, publically accessible source on the Internet for a period of 6 months. Microsoft will also effect notice by additional methods as may be directed by the Court.

Notice and service by the foregoing means satisfy Due Process, are appropriate, sufficient and reasonable to apprise Defendants of this action and are necessary under the circumstances. Microsoft hereby formally requests that the Court approve and order the alternative means of service discussed above.

First, legal notice and service by e-mail, facsimile, mail and publication satisfies Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing and the lawsuit. *See Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See e.g. Rio Properties, Inc. v. Rio Int'l.*



Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

*Interlink*, 284 F.3d 1007, 1014-1015 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); *Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) at Dkt. 38, pg 4, submitted at Cox Decl., ¶ 15, Ex. 13 (authorizing notice of preliminary injunction and service on botnet operators by e-mail, facsimile, mail and publication); *Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS 21712 (S.D.N.Y. 2001) (authorizing service by publication upon Osama bin Laden and the al-Qaeda organization); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535036 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products North Am., Inc. v Dagra*, 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, *3 (D. Md. 2010) (granting *ex parte* TRO and order prompting "notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or delivery services.").

Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit recently observed:

> [Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is e-mail-the method of communication which [Defendant] utilizes and prefers. In addition, e-mail was the only court-ordered method of service aimed directly and instantly at [Defendant] ... Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, e-mail may be the only means of effecting service of process.

*Rio Properties, Inc.*, 284 F.3d at 1014-1015; *see also Williams-Sonoma, Inc. v. Friendfinder, Inc.*, 2007 U.S. Dist. LEXIS 31299, *5-6 (N.D. Cal. 2007) (service by e-mail consistent with Hague Convention and warranted in case involving misuse of Internet technology by international defendants). In this case, the e-mail addresses provided by Defendants to the hosting companies, in the course of obtaining services that support the botnet, are likely to be the most accurate and viable contact information and means of notice and service. Moreover, Defendants will expect notice regarding their use of the hosting providers'

services to operate their botnet by those means, as Defendants agreed to such in their hosting agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311 (1964) ("And it is settled ... that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether."). For these reasons, notice and service by e-mail and publication are warranted and necessary here.[8]

For all of the foregoing reasons, Microsoft respectfully requests that the Court enter the requested TRO, seizure order and order to show cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing and service of the complaint set forth herein meet Fed. R. Civ. Pro. 4(f)(3), satisfy Due Process and are reasonably calculated to notify Defendants of this action.

## III. CONCLUSION

For the reasons set forth herein, Microsoft respectfully requests that this Honorable Court grant its motion for a TRO, seizure order and order to show cause regarding a preliminary injunction. Microsoft further respectfully requests that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

[8] Additionally, if the physical addressees provided by Defendants to hosting companies turns out to be false and Defendants' whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *See BP Products North Am., Inc.,* 236 F.R.D. at 271 ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.")


Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

Dated: February 8, 2011.

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: _____

Jeffrey L. Cox (WSBA No. 37534)
jcox@orrick.com
Ranjit Narayanan (WSBA No. 40952)
rnarayanan@orrick.com

701 5th Avenue
Suite 5600
Seattle, WA 98104-7097
Telephone: +1-206-839-4300
Facsimile: +1-206-839-4301

Of counsel:
Gabriel M. Ramsey (*pro hac vice* application pending)
gramsey@orrick.com
Jacob M. Heath (*pro hac vice* application pending)
jheath@orrick.com

1000 Marsh Road
Menlo Park, CA 94025
Telephone: +1-650-614-7400
Facsimile: +1-650-614-7401

Attorneys for Plaintiff Microsoft Corp.